나무위키

모네로

최근 수정 시각: 2026-08-04 13:47:20

분류:암호화폐 | 2014년 출시

목차

1. 개요
2. 익명성
   2.1. 익명성 깨짐
3. 채굴
4. 구매하는 방법
5. 핫 월렛과 콜드 월렛
6. 돈세탁?
7. 포크
8. 지갑 소프트웨어
9. Bytecoin
10. 취급 거래소
11. 사건·사고
12. 참고자료
13. 같이 보기

모네로 Monero	
MONERO	
ISO 4217 코드	XMR
중앙은행	없음
도입일	2014년 4월 18일
사용국	전 세계
분류	암호화폐
기호	ɱ[1]
발행 방식	PoW(Proof-of-Work, 작업 증명)
현재 발행량	18,446,744.07 XMR [2]
와이즈 레이팅스	C
개발 언어	C++
MONERO	

1. 개요

오픈 소스 P2P 암호화폐 중 하나다. 모네로(Monero)라는 이름은 에스페란토어로 동전을 뜻한다.#[3]

후술할 익명성 때문에 검은 돈이라는 면이 짙으며, 피해자의 컴퓨터에 암호화폐를 채굴하는 악성코드를 주입하는 크립토재킹 전용 암호화폐의 모습으로도 간간이 보인다.

사이트에서 XMR란을 체크하고 Filter를 클릭하면 KYC(Know Your Customer)를 요구하지 않으면서도 모네로 결제를 지원하는 상품을 찾아볼 수 있다.

2. 익명성

익명성에 초점을 둔 게 특징이다. 기존 프로토콜을 기반으로 하는 비트코인은 블록체인에 보내는 사람과 받는 사람이 투명하게 기록되거나 이용자의 IP가 남기 때문에 일반적인 이미지와는 달리 의외로 익명성 면에서 뒤떨어진다. 반면 모네로는 크립토노트(CryptoNote) 프로토콜로 송금증명을 채택하여 사용자의 익명성을 보호한다. 이 프로토콜의 작동 원리에 대해서는 여기를 참고.

거래가 시작되면 특정 그룹 내에서 키가 섞이는 링 시그니처(ring signature)라는 기술을 사용한다. 이 그룹 내의 거래 내역을 조회하려면 private key가 필요해서 private key가 없이는 누가 누구에게 얼마를 보냈는지를 알 수 없다.

또한 토르 네트워크를 통한 서비스도 진행중이다.

또, 모네로는 I2P를 사용하여 거래자의 IP 주소를 숨길 수 있는 Kovri 프로젝트를 개발 중이다.

비슷하게 익명성을 중시한 암호화폐로는 라이트코인, Zcash, Dash 등이 있다.

모네로를 송금할 때는 자신의 개인지갑에서 상대방의 개인지갑으로(개인지갑->개인지갑) 송금한다. 거래소지갑에서 상대방에게 바로 송금할 경우(거래소지갑->개인지갑) 거래내용을 거래소가 알 수 있기 때문이다.[4] 기본적으로 거래소를 믿지 않는다. "Not your keys, not your coins."를 명심한다.

모네로 지갑의 주소에는 '4'로 시작하는 기본 주소(Primary Address)와 '8'로 시작하는 서브 주소(Sub Address)가 있다. 기본 주소(Primary Address)는 사용하지 않고 서브 주소(Sub Address)를 대신 사용하는 것이 프라이버시와 익명성에 더 좋다. 서브 주소(Sub Address)의 역할 중 하나는 신원을 분리하는 것이다. 인터넷상에서 활동 A와 활동 B를 할 때 신원을 분리하고 싶다면 서로 다른 서브 주소(Sub Address)를 사용해야 한다.

모든 활동을 하나의 모네로 지갑 주소로 하면 신원을 특정당할 위험이 생길 수 있다. 비유하자면, 만약 네이버 아이디와 인터넷 커뮤니티의 아이디가 똑같다면 약간의 조사만으로도 네이버 계정이 드러남은 물론 신원이 노출될 수 있다. 네이버 아이디와 인터넷 커뮤니티의 아이디를 다르게 만들면 이런 신원 추적을 방지할 수 있다. 마찬가지로 모네로로 돈을 받게 되는 상황이 오면 상대방에게 내 모네로 주소를 알려줘야 하는데, 여러 활동을 하면서 하나의 모네로 주소만 쓴다면 신원을 특정당할 가능성이 생기게 된다. 예를 들어 철수가 친구 영희에게 모네로로 돈을 받을 때 영희에게 8abcdefg라는 주소를 알려주었고, 인터넷상에서 다른 활동을 할 때 8abcdefg이라는 주소를 게시했다고 가정하면, 영희는 철수가 인터넷에서 어떤 활동을 하는지 알 수 있다.

이때 서브 주소(Sub Address)를 활용한다면 신원 추적의 가능성을 줄일 수 있다. 예를 들어 철수가 친구 영희에게 모네로로 돈을 받을 때 영희에게 8abcdefg라는 주소를 알려주었고, 인터넷상에서 다른 활동을 할 때 8hijklmn이라는 주소를 게시했다고 가정하면, 영희는 철수가 인터넷에서 어떤 활동을 했는지 알 수 없다.
단 정말 위험한 거래는 별도의 지갑을 만드는 것이 더 안전하다.#

공개적인 장소에 자신의 모네로 개인키, 트랜잭션 ID, 거래 시간, 거래 금액을 게시하지 않는다.

2.1. 익명성 깨짐

보안 취약점으로 상당수 거래의 거래 액수와 발신(송금) 주소가 추적 가능하게 되었었지만 현재는 수정되었다고 한다. 그러 수신 주소는 추적이 안 된다고 한다.

Litecoin Dark Web Adoption Rises as Monero Privacy Flaw is Exposed(MAR 28, 2018)

3. 채굴

모네로는 사토시 나카모토가 비트코인의 PoW를 설계할때 있었던 철학처럼 one-CPU-one-vote 철학을 따르기 위해서 ASIC은 물론 GPU까지 강하게 막으면서 CPU 친화적 채굴 환경을 제공한다.[5] 기존에는 CryptoNight라는 CPU에 최적화되고 ASIC과 GPU에 저항성이 강한 특유의 PoW 채굴 방식을 사용했으나 ASIC 제작사들이 CryptoNight 채굴에 최적화된 CryptoNight ASIC을 선보이면서 채굴의 중앙화 우려가 생겼고 아예 CryptoNight와는 시스템 자체가 다른 R

andomX 채굴 방식을 개발했다, RandomX는 ASIC 저항성이 매우 강하고 CPU에 훨씬 더 최적화된 채굴 방식이다 그리고 모네로의 채굴 방식은 매우 다양한데 그 방법 중 하나가 안타깝게도 크립토재킹이다... 모네로는 특유의 익명성과 커뮤니티적 특성으로 크립토재킹 멀웨어에 사용하기에 매우 최적인 데다가 대부분의 컴퓨터가 GPU는 없더라도 CPU는 거의 다 있으니 더 최적화된 것이다. 그래서 공격자는 전기세, 유지비가 전혀 없이 채굴 보상을 받으니 채굴 경쟁의 출발점부터가 달라서 모네로의 전체적 채굴 수익에 꽤 영향을 주긴 할 것이다. 하지만 궁극적으로는 모네로의 채굴 수익은 형편없다. 특히 전기세가 비싼 한국에서는 채굴을 하면 할수록 전기세로 돈을 내야 하는 구조다. 초고효율 고성능 CPU로 전기세가 낮은 곳에서 채굴하지 않는 이상 수익률은 별로 좋지가 않아서 소규모 채굴자가 많은 구조이다. 그리고 모네로의특성상 채굴 풀도 종류가 매우 다양하다.

4. 구매하는 방법

아래의 글은 모네로를 구하는 방법 중 하나이다. 모네로를 구하는 방법에는 여러 가지가 있다.

1. 기존 통장(원화) -> 케이뱅크(원화) -> 업비트(원화) -> 업비트(XRP(구 Ripple)) -> 바이낸스(XRP(구 Ripple)) -> 바이낸스(Litecoin(LTC)) -> Cake Wallet(Litecoin(LTC)) -> Cake Wallet(Monero(XMR)) -> Monero.com(Monero(XMR)) or Feather Wallet(Monero(XMR))

2. 기존 통장(원화) -> 케이뱅크(원화) -> 업비트(원화) -> 업비트(수이(암호화폐)[6] -> 자신의 개인지갑[7]으로 수이를 출금한다. -> 체인지나우에서 수이를 모네로로 스왑한다.[8] -> 최저 슬리피지, 최저수수료, 탈중앙화[9]를 누리면서 편하게 모네로를 구매할 수 있다. 처음에 업비트, 빗썸 같은 중앙화 거래소를 거치는 건 1번의 방법과 같지만 그 이후의 과정이 DEX와 안전한 개인 지갑으로 이루어지고 과정이 훨씬 간단하다.
다른 코인으로 모네로를 구하고자 할 때 수수료가 싸고 전송 속도가 빠른 Litecoin(LTC)를 이용하는 것을 권장한다. Litecoin(LTC)은 한국 거래소에서 상장폐지되었으므로 수수료가 싸고 전송 속도가 빠른 Ripple(XRP)을 국내 거래소에서 구해서 해외 거래소로 보낸 뒤 Litecoin(LTC)으로 교환하여 구한다. 관련글 @[10]

Cake Wallet에서 만들 수 있는 코인 지갑은 Monero(XMR), Bitcoin(BTC), Ethereum(ETH), Litecoin(LTC), Bitcoin Cash(BCH), Polygon(MATIC), Nano(XNO), Haven(XHV)[11] 총 8개이다.

Tails OS의 Persistent Storage에 모네로 지갑을 설치하고 거기에 모네로를 보관하는 것이 가장 안전하다.[12] 모네로 지갑용 Tails OS USB로 모네로 지갑 외 다른 활동은 하지 않는다. 이는 만에하나 웹서핑 등 다른 활등을 하는 과정에서 악성코드에 감염되어서 모네로 지갑이 해킹당할 가능성을 사전에 방지하기 위해서이다.
만약 자신의 위협 모델(Threat Model)이 편의성을 위해 프라이버시와 익명성을 조금 포기해도 될 정도이고, 모네로로 결제하기 위해 매번 PC를 켜야 하는 것이 번거롭다고 생각하며, 큰 돈이 아닌 소액만 취급한다면 Monero.com을 대신 사용해도 된다. 단 가급적이면 모네로 공식 지갑이나 Feather Wallet을 사용하기를 권장한다.

하나의 개인 지갑에서 다른 모네로 개인 지갑으로 전송하는 과정(10번)은 번거롭게 느낄 수 있더라도 반드시 해야 한다. #

동영상에서 레퍼럴이니 선물거래니 하는 건 전부 무시하고 스킵해도 된다. 모네로 구입에 전혀 필요없다.

1. 먼저 코인을 구매할 거래소에 대해서 알아야 한다. 아래 과정은 업비트를 기준으로 진행한다.

오류가 발생했습니다.

www.youtube.com에서 동영상을 시청하거나 브라우저에서 자바스크립트가 사용 중지된 경우 사용 설정하세요.

2. 케이뱅크와 업비트에 가입한다.

오류가 발생했습니다.

www.youtube.com에서 동영상을 시청하거나 브라우저에서 자바스크립트가 사용 중지된 경우 사용 설정하세요.

3. 업비트에서 Ripple(XRP)을 산다.

4. 바이낸스에 가입한다.

5. 업비트의 Ripple(XRP)을 바이낸스로 전송한다.

6. 바이낸스에서 Ripple(XRP)을 Litecoin(LTC)으로 교환한다.

7. Cake Wallet을 설치하고 Monero(XMR) 지갑과 Litecoin(LTC) 지갑을 만든다.

8. 바이낸스의 Litecoin(LTC)을 Cake Wallet으로 전송한다.

9. Cake Wallet에서 Litecoin(LTC)을 Monero(XMR)로 교환한다.

10. Cake Wallet의 Monero(XMR)를 Monero.com 또는 Feather Wallet으로 전송한다.

11. 이제 Monero(XMR)로 원하는 것을 구매한다.

다들 모네로를 통해 검열없는 금융 프라이버시를 누리길 바란다.

5. 핫 월렛과 콜드 월렛

🔗 https://www.reddit.com/r/Monero/comments/12d77tb/creating_reasonably_secure_monero_hot_wallets_and/
🔗 @
🔗 https://hackernoon.com/my-crypto-wallet-setup-lets-me-stay-anonymous-while-protecting-me-against-theft
🔗 @
🔗 https://malvarma.org/

Tails OS에서 모네로 Hot Wallet(Feather Wallet)을 만드는 영상

핫 월렛(Hot Wallet)은 인터넷에 연결된 지갑이고 콜드 월렛(Cold Wallet)은 인터넷에 연결되지 않은 지갑이다. 콜드 월렛은 핫 월렛보다 보안상 더 안전하다는 장점이 있지만 지갑을 만드는 방법과 거래하는 방법이 핫 월렛보다 더 어렵다는 단점이 있다.

모네로 공식 지갑과 Feather Wallet 둘 다 핫 월렛 방식으로도 콜드 월렛 방식으로도 만들 수 있다. 지갑을 만들거나 거래를 할 때 인터넷에 연결하지 않으면 그것이 바로 콜드 월렛이다.

위협 모델(Threat Model)이 매우 강력한 상황이 아니라면 Tails OS에서 핫 월렛을 만드는 것만으로도 대부분 사람들에게는 충분하다.

6. 돈세탁?

> **Money laundering in the modern era is hard and hackers aren't inherently better at it than anyone else.** In the modern connected world, money always comes from somewhere and it always goes somewhere. Banks in most countries are under strict Know Your Customer (KYC) laws and those that aren't usually still do business in America and so their American branches are. America has also punished international banks for overseas behavior by fining their American subsidiaries. (This is how most sanctions are actually implemented. **If you want to work in US dollars, you're basically subjected to US banking regulations.**)
> Cryptocurrencies are popular for this, but most cryptocurrencies are actually very bad at money laundering because they create an immutable record. **There are some privacy-oriented cryptos which are better about this (monero and Zcash), but they have liquidity/exit problems. Hackers can't use a centralized exchange**, since again, most of them are under KYC requirements or if the hacker tries to cash out, their US-transacting bank is. So basically, the way most hackers clean their money is by avoiding the need to do so. **Hackers will keep their**

proceeds (or themselves) in countries with lax AML and KYC requirements. This is why the majority of criminal hackers who are in it for the money are based in places like Russia.
Hackers don't magically have great technological solutions to working around social systems.
Once again, **changing that money(cryptocurrency) into dollars will mean working with a bank that does dollar clearing transactions. Unless you are working in comparatively small amounts of money that go below reporting thresholds, you're going to get caught doing this eventually.**
Doing it in Dubai specifically at any major international bank would probably raise more flags since they're on FATF's list of countries at increased risk for money laundering. Also, brushing by "through foreign companies" hides an awful lot. Which foreign companies. **Are these "foreign companies" multinationals? If so, then they probably have a lot of the same AML, KYC, and financial crimes requirements as US companies.**
Heck, even getting to Dubai to do this (unless the person in question is doing their hacking from the UAE) is a problem. **A fact pattern of "this person flew to Dubai and suddenly got much richer" is suspicious on its own.**
What's more, **just the BTC->XMR->BTC change isn't enough. This is susceptible to correlation attacks. If, say, a ransom of a certain amount gets paid out to a specific set of addresses, and then transfers on an exchange are seen in those exact same amounts to another set of BTC addresses, then that's evidence that those addresses are connected, even if the XMR transaction in the middle is anonymous, as far as we currently know.**
Like I said in my original post, **keeping money in countries with poor AML laws is one way around this.** If a person wants to do their hacking strictly from the UAE and keep their money in Dirham, then that might work, but **moving large amounts of it into dollars is going to be complicated on a scale far beyond just using "foreign companies" to "[invest] around the world".**
Being a hacker who commits crimes for money is harder in the US, for sure.
As for Russia, I mean, I'm sure they have some, but they are likely weaker than the US and they lack the US's super-weapon: control of the global reserve currency. **US-denominated transactions always end up with more scrutiny than other transactions because the US has more control over international institutions.**
(Russia has one other thing going for it for criminal hackers in that they tend not to prosecute digital crimes committed against entities outside their borders.)
For specifically countries with especially weak money-laundering laws, the FATF keeps a black list and gray list.
https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html

현대 사회에서 자금 세탁은 어렵고 해커들이 다른 사람들보다 본질적으로 더 잘하는 것은 아닙니다. 현대의 연결된 세상에서 돈은 항상 어딘가에서 나오고 어딘가로 갑니다. 대부분의 국가 은행은 엄격한 고객 신원 확인(KYC) 법률을 준수해야 하며, 그렇지 않은 은행들은 대개 미국에서 사업을 하고 있기 때문에 미국 지점도 마찬가지입니다. 미국은 해외에서 활동하는 외국 은행에 미국 자회사에 벌금을 부과하여 처벌하기도 합니다. (대부분의 제재가 실제로 시행되는 방식입니다. **미국 달러로 거래하려면 기본적으로 미국 은행 규제를 따라야 합니다.**)
암호화폐는 이러한 이유로 인기가 있지만, 대부분의 암호화폐는 불변의 기록을 생성하기 때문에 자금 세탁에 매우 취약합니다. **모네로와 Zcash처럼 개인정보 보호에 중점을 둔 암호화폐는 이러한 측면에서 더 우수하지만, 유동성/출금 문제가 있습니다. 해커는 중앙화된 거래소(CEX)를 사용할 수 없습니다.** 대부분의 거래소는 KYC 요건을 준수해야 하거나, 해커가 현금화를 시도하면 미국 거래 은행이 해당 요건을 충족해야 하기 때문입니다.
기본적으로 대부분의 해커들은 자금 세탁의 필요성을 회피하는 방식으로 자금을 세탁합니다. **해커들은 자금세탁방지(AML) 및 고객알기제도(KYC) 요건이 느슨한 국가에 자금(또는 자신)을 보관합니다. 이것이 바로 돈을 노리는 범죄 해커들의 대부분이 러시아와 같은 곳에 기반을 둔 이유입니다.**
해커들이 사회 시스템을 우회할 수 있는 마법 같은 기술적 해결책을 가지고 있지는 않습니다.
다시 한번 말하지만, **그 돈(암호화폐)을 달러로 환전하려면 달러 청산 거래를 하는 은행과 협력해야 합니다. 보고 기준치 이하의 비교적 소액 자금을 다루는 경우가 아니라면, 결국 이런 행위를 하다 적발될 것입니다.**
특히 두바이의 주요 국제 은행에서 이런 행위를 한다면 FATF의 자금세탁 위험 증가 국가 목록에 올라 있기 때문에 더 큰 문제가 될 것입니다. 또한 "외국 기업을 통해" 스쳐 지나가는 행위에는 많은 것이 숨겨져 있습니다. 어떤 외국 기업인가요? **이 "외국 기업"들이 다국적 기업인가요? 그렇다면 미국 기업과 동일한 AML, KYC, 금융 범죄 요건을 갖추고 있을 가능성이 높습니다.**
심지어 두바이까지 가서 해킹을 하는 것조차 문제입니다(해당 인물이 UAE에서 해킹을 하는 것이 아니라면). **"이 사람이 두바이로 날아가 갑자기 훨씬 부자가 되었다"는 사실 자체만으로도 의심스럽습니다.**
게다가 **BTC->XMR->BTC로의 환전만으로는 충분하지 않습니다. 이는 상관관계 공격(correlation attack)에 취약합니다. 예를 들어 특정 주소에 일정 금액의 몸값이 지불된 후 거래소에서 동일한 금액이 다른 BTC 주소로 이체된다면, 현재 알려진 바에 따르면 중간의 XMR 거래가 익명이라 하더라도 해당 주소들이 서로 연결되어 있다는 증거가 됩니다.**
제가 원래 게시물에서 말씀드렸듯이, **AML 법률이 취약한 국가에 자금을 보관하는 것이 이를 우회하는 한 가지 방법입니다.** UAE에서만 해킹을 하고 돈을 디르함으로 보관하려는 사람이라면 그럴 수도 있겠지만, **막대한 금액을 달러로 환전하는 것은 단순히 "외국 기업"을 이용해 "전 세계에 투자"하는 것 이상으로 훨씬 더 복잡한 문제입니다.**
미국에서 돈을 노리고 범죄를 저지르는 해커는 분명 더 어려울 것입니다.
러시아의 경우, 물론 어느 정도 영향력은 있지만 미국보다 약할 가능성이 높고, 미국의 초강력 무기인 세계 기축통화 통제력이 부족합니다. **미국이 국제기구에 대한 통제력이 더 크기 때문에 미국 달러로 거래하는 것은 다른 거래보다 항상 더 엄격한 감시를 받습니다.**
(러시아는 국경 밖의 기관을 대상으로 한 디지털 범죄를 기소하지 않는 경향이 있다는 점에서 범죄 해커들에게 유리한 또 다른 장점이 있습니다.)
특히 자금세탁 방지법이 취약한 국가들을 위해 FATF는 블랙리스트와 그레이리스트를 운영하고 있습니다.
https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html

https://www.reddit.com/r/hacking/comments/15rb0mg/how_do_hackers_clean_their_money/

돈세탁에는 두 가지 요소가 있는데 하나는 돈의 출처를 숨기는 것이고 다른 하나는 돈의 출처를 거짓으로 꾸며내는 것이다. 그리고 모네로를 비롯한 어떤 프라이버시 코인도 돈의 출처를 거짓으로 꾸며내지는 못한다. 그러므로 단순히 프라이버시 코인을 구매했을 때의 과정을 거꾸로 하면 된다고 여겼다면 이는 안일한 생각이다. 출처를 알 수 없는 돈이 들어오는 사람을 가만히 내버려두는 나라는 전세계 어디에도 없다.

또한 프라이버시 코인을 이용하더라도 결국 돈을 실질적으로 쓰기 위해서는 현금으로 교환해야 하는데 이 과정에서 흔적이 남을 가능성이 매우 높다. 암호화폐로 상품을 직접 구매하는 것이 최선이지만 암호화폐를 받아주는 온라인 및 오프라인 상점은 극히 드물다.

7. 포크

최근 1,546,000블럭에서 하드포크가 진행되어[13] 모네로 오리지널(XMO)과 모네로(XMR)로 포크되었다.

이를 통해 Cryptonight V7으로 채굴 알고리즘이 바뀌었다.[14]

8. 지갑 소프트웨어

비트코인의 Bitcoin Core나 Electrum 같은 지갑 소프트웨어가 모네로에도 있다. 거래소는 위험하니 콜드 월렛에 알아서 잘 보관하자.

Monero GUI Wallet은 Bitcoin Core라고 생각하고 Feather wallet은 Electrum이라고 생각하면 편하다. 이래도 알기 어려우면 풀노드 월렛과 하프노드[15]라고 생각하면 된다. 그리고 대부분의 경우에는 Feather wallet이 훨씬 더 좋다.

Feather wallet 다운로드는 여기에서 받으면 되고 윈도우 이용자의 경우 윈도우 아이콘이 있는 항목에서 설치를 눌러서 설치하고 이용하면 된다.

다운로드는 여기[16]에서 받을 수 있다. Windows, macOS, Linux, ARM에서 사용 가능하다. 이 지갑에는 채굴 기능이 포함되어 있다. 모네로 제작자 공식 소프트웨어는 아니지만 블록체인 동기화가 필요없는 light wallet과 모바일용 지갑도 있다.

설치 방법은 다음 링크 참조.
윈도우에서 모네로 XMR 지갑 만들기 2017.08.28

9. Bytecoin

모네로가 사용하는 CryptoNote, ring signature, stealth address는 바이트코인(Bytecoin)에서 사용하던 기술이다. 바이트코인은 2012년에 만들어진 익명 코인이다. 모네로는 바이트코인의 포크로 2014년 4월에 생겼다.

모네로에는 ring CT라는 바이트코인에는 없던 새로운 익명 강화 기술이 추가되었다.

10. 취급 거래소

CoinMarketCap 시가총액 25위로 꽤 메이저한 알트코인이지만, 익명 거래가 금기시되는 한국의 법률 특성상 국내의 암호화폐 거래소에서는 2020년 이후 모두 상장폐지되었다. 2021년에는 특금법 개정에 따라 국내 거래소에서는 취급 자체가 불법화될 예정이다. 다만 소유 및 해외 거래소에서 사용하는 것은 불법이 아니기 때문에 모네로를 소유한 한국인들은 여전히 있다.

> 《특정 금융거래정보의 보고 및 이용 등에 관한 법률》
> 제8조(가상자산사업자의 조치) 가상자산사업자는 제4조제1항 및 제4조의2에 따른 보고의무 이행 등을 위하여 고객별 거래내역을 분리하여 관리하는 등 대통령령으로 정하는 조치를 하여야 한다.

> 《특정 금융거래정보의 보고 및 이용 등에 관한 법률 시행령》
> 제13조(가상자산사업자의 조치) 법 제8조에서 "대통령령으로 정하는 조치"란 다음 각 호의 조치를 말한다.
> 5. 가상자산이 하나의 가상자산 주소에서 다른 가상자산 주소로 이전될 때 전송기록이 식별될 수 없게 하는 기술이 내재된 가상자산을 취급하지 않도록 관리

게다가 미국에서도 2025년 7월 16~17일 지니어스, 클래리티 법안이 하원표결이 예정되어 있고, 특히 클래리티 법안 자체가 공화당과 민주당 사이에서 초당적 지지를 받는 법안이라 향후 2026년 초부터는 사실상 불법화될 예정이다.[17]

모네로 현물 거래가 가능한 나무위키에 문서가 존재하는 CEX

- KuCoin
- MEXC
- HTX
- Bitfinex
- Kraken

11. 사건·사고

- 2017년 12월, 해킹된 페이스북 메신저 계정을 통해 모네로 채굴 기능이 내장된 바이러스가 유포되는 사건이 발생하였다.(페이스북 메신저로 온 video.xxxx.zip 파일의 정체) 별도의 채굴 장비를 갖출 필요 없이 CPU만으로도 어느 정도 채산성을 확보할 수 있는 모네로의 특징을 악용한 사례. 이 점을 이용하여 이후에도 Drive-By-Mining이라 불리는, 스크립트를 이용하여 접속만으로 접속자의 리소스를 사용한 채굴하는 방법을 이용하는 해커들이 늘어나는 추세이다.
- 2018년 1월, 북한이 멀웨어를 이용한 해킹으로 모네로를 채굴한다는 보도가 나왔다. 위 사건과 연관되어 있는지는 후속 보도를 기다려야 할 듯.
- ~~불법 복제 Windows 10의 정품 인증을 해주는 프로그램 KMSpico에 프로그래머가 Monero 채굴 프로그램을 심어 놓았다.(윈도우 정품 인증 툴로 유명한 KMSpico, 가상화폐 채굴 악성코드 포함되어 있어)~~해당 기사는 공식 홈페이지가 아닌 변조 프로그램 사이트에서 받은 KMSpico다.[18]
- 유튜브 광고 플랫폼에서 JavaScript로 Monero를 채굴하는 광고가 발견되었다.(유튜브 광고에서 이용자 PC 가상화폐 채굴시키는 악성코드 발견)
- 심지어 게임으로 위장한 모네로 채굴 프로그램이 스팀에 나왔다가 내려갔다!!(#)
- 익명성 특화 코인이라는 점을 악용하여 범죄 자금의 돈세탁에 연루되기도 한다. 한국의 사례로는 n번방 사건(박사방)에서 "입장료"로 사용된 케이스[19]가 있다.
- 2022년 대러시아 경제제재에서 미국이 기존의 암호화폐인 비트코인 등을 러시아가 거래하지 못하게 제재대상에 올리는 것을 본격 추진하면서 대시 등 다른 거래가능 알트코인과 더불어 가격이 일정구간 올라갈 가능성이 생겼다. 모네로를 비롯해 상당수의 암호화폐가 추적이 아예 불가능하게 만들어져 있으면서도 발행제한이 있고 거래수단으로 받아들여지고 있기 때문이다. 물론 시가총액이 크지 않기 때문에 비트코인을 대체할 정도는 아니라지만, 베네수엘라도 대시라는 암호화폐로 어느 정도 화폐가치 폭락에 대응한 것을 볼 때 더욱 그렇다.
- 8월 14일, 큐빅은 모네로의 해시 파워의 과반이상을 장악하여 51% 공격에 위협이 있어 크라켄 거래소에서 출금이 일시중지되었다.

12. 참고자료

공개키 암호화와 PGP에 대한 소개
모네로 거래 및 보관 가이드
모네로 OPSEC 가이드 1편
모네로 OPSEC 가이드 2편
모네로 공식 GUI 지갑 만들기
모네로 Feather Wallet 만들기
윈도우에서 토르브라우저를 이용하여 다른 프로그램이 토르로 연결되도록 설정하는 방법
Privacy Guides - Cryptocurrency

13. 같이 보기

- 암호화폐
- Zcash

이 저작물은 CC BY-NC-SA 2.0 KR에 따라 이용할 수 있습니다. (단, 라이선스가 명시된 일부 문서 및 삽화 제외)
기여하신 문서의 저작권은 각 기여자에게 있으며, 각 기여자는 기여하신 부분의 저작권을 갖습니다.

나무위키는 백과사전이 아니며 검증되지 않았거나, 편향적이거나, 잘못된 서술이 있을 수 있습니다.
나무위키는 위키위키입니다. 여러분이 직접 문서를 고칠 수 있으며, 다른 사람의 의견을 원할 경우 직접 토론을 발제할 수 있습니다.